Doubles sommes de Sylvester et sous-résultants

Marie-Françoise Roy, Aviva Szpirglas

Doubles sommes de Sylvester et sous-résultants

Marie-Françoise Roy[1], Aviva Szpirglas[2]

21 décembre 2009

Table des matières

[1] IRMAR, UMR CNRS 6625, Université de Rennes 1.
[2] LMA, UMR CNRS 6086, Université de Poitiers.

1 Définitions et résultat principal.

Nous définissons les doubles sommes de Sylvester et les sous-résultants et donnons quelques unes de leurs propriétés.
Le résultat principal de l'article est de préciser les relations entre ces deux notions.
Soient $\mathbf{A}$ et $\mathbf{B}$ deux familles finies d'éléments d'un corps K, de cardinalité m et n ; on définit le *résultant de* $\mathbf{A}$ *et* $\mathbf{B}$ par

$$R(\mathbf{A},\mathbf{B}) := \prod_{a\in\mathbf{A},b\in\mathbf{B}} (a-b).$$

Notons que si $\mathbf{A}\cap\mathbf{B}\neq\emptyset$,

$$R(\mathbf{A},\mathbf{B}) = 0,$$

que

$$R(\mathbf{A},\emptyset) = 1,$$

et que

$$R(X,\mathbf{A}\cap\mathbf{B}) = \gcd(R(X,\mathbf{A}),R(X,\mathbf{B})).$$

1.1 Doubles sommes de Sylvester.

Si $\mathbf{A}$ est un ensemble fini et $\mathbf{C}$ est un sous-ensemble de $\mathbf{A}$ de cardinalité p, on utilisera la notation. $\mathbf{C}\subset_p\mathbf{C}$.
Si $\mathbf{A}$ et $\mathbf{B}$ sont deux ensembles finis et p et q deux entiers vérifiant $p+q\leq\min(\#\mathbf{B},\#\mathbf{A})$, on définit la *double somme de Sylvester d'exposant* (p,q), notée $\mathrm{Sylv}^{p,q}$, par

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X) := \sum_{\substack{\mathbf{C}\subset_p\mathbf{A}\\ \mathbf{D}\subset_q\mathbf{B}}} R(X,\mathbf{C})R(X,\mathbf{D})\frac{R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})}.$$

Remarque 1.1 Les doubles sommes de Sylvester ont les propriétés suivantes.

1. Le degré de $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X)$ par rapport à X est $\leq p+q$.
2. $\mathrm{Sylv}^{0.0}(\mathbf{A},\mathbf{B})(X) = R(\mathbf{A},\mathbf{B})$.
3. Les double sommes de Sylvester non nulles de plus petit degré sont un pgcd de $R(X,\mathbf{A})$ et $R(X,\mathbf{B})$. Plus précisément, si j est le nombre d'éléments de $\mathbf{A}\cap\mathbf{B}$,
   (a) pour tous p,q tels que $j=p+q$, $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X)$ est un pgcd de $R(X,\mathbf{A})$ et $R(X,\mathbf{B})$,
   (b) pour tous p,q tels que $j>p+q$, $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X)=0$.

Les propriétés 1 et 2 sont vraies par définition. Les propriétés 3(a) et 3(b) proviennent du fait que si $\sharp(\mathbf{C})=p,\sharp(\mathbf{D})=q$,
– si $p+q=\sharp(\mathbf{A}\cap\mathbf{B})$, $\mathbf{C}\cup\mathbf{D}=\mathbf{A}\cap\mathbf{B}$,

$$R(X,\mathbf{C})R(X,\mathbf{D}) = R(X,\mathbf{A}\cap\mathbf{B}) = \gcd(R(X,\mathbf{A}),R(X,\mathbf{B})),$$

– si ($p+q=\sharp(\mathbf{A}\cap\mathbf{B})$ et $\mathbf{C}\cup\mathbf{D}\neq\mathbf{A}\cap\mathbf{B}$) ou si $p+q<\sharp(\mathbf{A}\cap\mathbf{B})$,

$$R(\mathbf{A}\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D}) = 0,$$

puisque $(\mathbf{A}\setminus\mathbf{C})\cap(\mathbf{B}\setminus\mathbf{D})\neq\emptyset$.

1.2 Sous-résultants.

Soient A et B deux polynômes unitaires de degré respectif m et n, avec $n < m$.

$$A = \sum_{k=0}^{m} \alpha_k X^{m-k} \quad B = \sum_{k=0}^{n} \beta_k X^{n-k}.$$

Pour $j \leq n-1$, $\mathrm{Sylv}_j(A,B)$ désigne la matrice dont les lignes sont les coordonnées des polynômes $X^{n-1-j}A, \ldots, A, B, \ldots, X^{m-1-j}B$ (dans cet ordre), dans la base $\{X^{m+n-j-1}, \ldots, 1\}$ de $K[X]$. C'est une matrice d'ordre $(m+n-2j) \times (m+n-j)$.
Pour $j \leq n-1$, le *sous-résultant d'indice* j de A et B, noté $\mathrm{Sres}_j(A,B)(X)$, est le déterminant de la matrice $M_j(A,B)$, dont les $(m+n-2j-1)$ premières colonnes sont celles de $\mathrm{Sylv}_j(A,B)$, la dernière (la $(m+n-2j)$-ième) est formée des polynômes $X^{n-1-j}A, \ldots, A,\ B, \ldots, X^{m-1-j}B$ (dans cet ordre). On a donc

$$\mathrm{Sres}_j(A,B)(X) = \begin{vmatrix} 1 & \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_{m+n-2j-2} & X^{n-j-1}A \\ 0 & 1 & \alpha_1 & \alpha_2 & \cdots & \alpha_{m+n-2j-3} & X^{n-j-2}A \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \bullet & \bullet & \bullet & \bullet & \cdots & \alpha_{m-j-1} & A \\ \bullet & \bullet & \bullet & \bullet & \cdots & \beta_{n-j-1} & B \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & \beta_1 & \beta_2 & \cdots & \beta_{m+n-2j-3} & X^{m-j-2}B \\ 1 & \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{m+n-2j-2} & X^{m-j-1}B \end{vmatrix}$$

avec la convention : $\alpha_i = 0$ pour $i > m$ et $\beta_i = 0$ pour $i > n$. Soit, pour $k \leq j$, $\mu_{k,j}(A,B)$ le mineur d'ordre $(m+n-2j) \times (m+n-2j)$ extrait de $\mathrm{Sylv}_j(A,B)$ construit sur les $m+n-2j-1$ premières colonnes et la $(m+n-j-k)$-ième colonne. Alors, en développant le déterminant de la matrice $M_j(A,B)$ par rapport à sa dernière colonne, on trouve

$$\mathrm{Sres}_j(A,B)(X) = \sum_{k=0}^{j} \mu_{k,j} X^k.$$

On définit $\varepsilon_k = (-1)^{[k/2]} = (-1)^{k(k-1)/2}$.

Remarque 1.2 Les sous-résultants ont les propriétés suivantes.

1. Le sous-résultant $\mathrm{Sres}_j(A,B)(X)$ est un polynôme de degré $\leq j$.
2. $\mathrm{Sres}_0(A,B)(X) = \varepsilon_m R(\mathbf{A},\mathbf{B})$, où $\mathbf{A}$ et $\mathbf{B}$ sont les deux familles finies données par les racines de A et de B dans un corps algébriquement clos contenant K.
3. Le sous-résultant non nul de plus petit degré est un pgcd de A et B.
4. Pour tout C polynôme de degré c,

$$\mathrm{Sres}_{j+c}(AC,BC)(X) = C(X)\mathrm{Sres}_j(A,B)(X).$$

Les trois premières propriétés sont similaires à celles des doubles sommes de Sylvester notées dans la remarque 1.1, leurs démonstrations sont données dans [2]. La dernière propriété se montre *via* un calcul de déterminant.

1.3 Le résultat principal.

Soient A et B deux polynômes unitaires de degrés respectifs m et n, et $\mathbf{A}$ et $\mathbf{B}$ les deux familles finies données par les racines de A et de B dans un corps algébriquement clos contenant K. On a

$$A = R(X, \mathbf{A}) \quad , \quad B = R(X, \mathbf{B}).$$

Le résultat principal de l'article est l'égalité (à une constante près) entre les sous-résultants de A et B et les doubles sommes de Sylvester des familles $\mathbf{A}$ et $\mathbf{B}$.

Théorème principal. *Soit $j \leq n < m$; pour tous p, q tels que $p + q = j$, $\mathrm{Sres}_j(A, B)(X)$ et $\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(X)$ sont égaux à une constante près. Plus précisément,*

$$(-1)^{p(m-j)}\varepsilon_{m-j}\binom{j}{p}\,\mathrm{Sres}_j(A, B)(X) = \mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(X).$$

Ce théorème, énoncé par Sylvester, est prouvé dans [4], ainsi que dans [1]. La preuve de [4] s'appuie sur les fonctions de Schur, les multifonctions de Schur et leurs propriétés. La preuve de [1] travaille avec des matrices. Nous présentons une preuve simple par récurrence sur n.

2 Deux propriétés des sommes de Sylvester.

Nous redonnons ici les démonstrations de deux propriétés des sommes de Sylvester (voir [4]).

Soit $\mathbf{A}$ un ensemble fini d'éléments d'un corps. Si $a \in \mathbf{A}$, on note a l'ensemble $\{a\}$ et $\mathbf{A} \setminus a$ l'ensemble $\mathbf{A} \setminus \{a\}$.
Pour tout polynôme A, on note $\mathbf{c}_j(A)$ le coefficient du terme de degré j de A.

Proposition 2.1 *Soient $j < n < m$; pour tous p, q tels que $j = p + q$, et $b \in \mathbf{B}$;*

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(b) = (-1)^{m-j}A(b)\mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B} \setminus b)(X))$$

Preuve.

$$\begin{aligned}
\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(b) &= \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \\ \mathbf{D} \subset_q \mathbf{B}}} R(b, \mathbf{C})R(b, \mathbf{D})\frac{R(\mathbf{C}, \mathbf{D})R(\mathbf{A} \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D})}{R(\mathbf{C}, \mathbf{A} \setminus \mathbf{C})R(\mathbf{D}, \mathbf{B} \setminus \mathbf{D})} \\
&= (-1)^{m-j}A(b) \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \\ \mathbf{D} \subset_q \mathbf{B}}} \frac{R(\mathbf{C}, \mathbf{D})R(\mathbf{A} \setminus \mathbf{C}, (\mathbf{B} \setminus b) \setminus \mathbf{D})}{R(\mathbf{C}, \mathbf{A} \setminus \mathbf{C})R(\mathbf{D}, (\mathbf{B} \setminus b) \setminus \mathbf{D})}
\end{aligned}$$

En effet, si $b \in \mathbf{D}$, alors, tous les termes qui contiennent $R(b, \mathbf{D})$ sont nuls ; si $b \notin \mathbf{D}$, alors

$$\begin{aligned}
R(b, \mathbf{C})R(\mathbf{A} \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D}) &= (-1)^{m-p}A(b)R(\mathbf{A} \setminus \mathbf{C}, (\mathbf{B} \setminus b) \setminus \mathbf{D}), \\
\tfrac{R(b,\mathbf{D})}{R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})} &= (-1)^q \tfrac{1}{R(\mathbf{D},(\mathbf{B}\setminus b)\setminus\mathbf{D})}
\end{aligned}$$

Ce qui donne le résultat, car le coefficient de degré j de $\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B} \setminus b)(X)$ est

$$\sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \\ \mathbf{D} \subset_q \mathbf{B} \setminus b}} \frac{R(\mathbf{C}, \mathbf{D})R(\mathbf{A} \setminus \mathbf{C}, (\mathbf{B} \setminus b) \setminus \mathbf{D})}{R(\mathbf{C}, \mathbf{A} \setminus \mathbf{C})R(\mathbf{D}, (\mathbf{B} \setminus b) \setminus \mathbf{D}).}$$

∎

Proposition 2.2

1. *Si $n < m$ et $p + q = n$, alors*

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(X) = (-1)^{p(m-n)} \binom{n}{p} B(X).$$

2. *Si $n = m = p + q$, alors*

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(X) = \binom{n-1}{q} A(X) + \binom{n-1}{p} B(X).$$

La preuve de la proposition 2.2 utilise le lemme suivant.

Lemme 2.3

1. *Soient $j \leq n < m$; pour tous p, q tels que $j = p + q$, et $a \in \mathbf{A}$;*

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(a) = (-1)^p B(a) \mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A} \setminus a, \mathbf{B})(X))$$

2. *Soient $j = n = m$; pour tous p, q tels que $j = p + q$, Si $q \neq 0$, pour tout $a \in \mathbf{A}$;*

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(a) = (-1)^p B(a) \mathbf{c}_{j-1}(\mathrm{Sylv}^{p,q-1}(\mathbf{B}, \mathbf{A} \setminus a)(X))$$

3. *Soient $j = n = m$; pour tous p, q tels que $j = p + q$, Si $p \neq 0$, pour tout $b \in \mathbf{B}$;*

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(b) = (-1)^q A(b) \mathbf{c}_{j-1}(\mathrm{Sylv}^{q,p-1}(\mathbf{A}, \mathbf{B} \setminus b)(X))$$

Preuve.

1. $j \leq n < m$. On remarque que $p < m$.

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(a) = \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \setminus a \\ \mathbf{D} \subset_q \mathbf{B}}} R(a, \mathbf{C}) R(a, \mathbf{D}) \frac{R(\mathbf{C}, \mathbf{D}) R(\mathbf{A} \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D})}{R(\mathbf{C}, \mathbf{A} \setminus \mathbf{C}) R(\mathbf{D}, \mathbf{B} \setminus \mathbf{D})}$$

Or,

$$R(\mathbf{A} \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D}) = R(a, \mathbf{B} \setminus \mathbf{D}) R((\mathbf{A} \setminus a) \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D}),$$
$$R(\mathbf{C}, \mathbf{A} \setminus \mathbf{C}) = R(\mathbf{C}, (\mathbf{A} \setminus a) \setminus \mathbf{C}) R(\mathbf{C}, a).$$

D'où

$$\begin{aligned}
\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B})(a) &= B(a) \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \setminus a \\ \mathbf{D} \subset_q \mathbf{B}}} \frac{R(a, \mathbf{C}) R(\mathbf{C}, \mathbf{D}) R((\mathbf{A} \setminus a) \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D})}{R(\mathbf{C}, (\mathbf{A} \setminus a) \setminus \mathbf{C}) R(a, \mathbf{C}) (-1)^p R(\mathbf{D}, \mathbf{B} \setminus \mathbf{D})} \\
&= B(a)(-1)^p \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \setminus a \\ \mathbf{D} \subset_q \mathbf{B}}} \frac{R(\mathbf{C}, \mathbf{D}) R((\mathbf{A} \setminus a) \setminus \mathbf{C}, \mathbf{B} \setminus \mathbf{D})}{R(\mathbf{C}, (\mathbf{A} \setminus a) \setminus \mathbf{C}) R(\mathbf{D}, \mathbf{B} \setminus \mathbf{D})} \\
&= B(a)(-1)^p \mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A} \setminus a, \mathbf{B})(X))
\end{aligned}$$

2. $j = n = m = p + q$.

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \setminus a \\ \mathbf{D} \subset_q \mathbf{B}}} \frac{R(a,\mathbf{C})R(a,\mathbf{D})R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})}$$

Posons

$$M = \frac{R(a,\mathbf{C})R(a,\mathbf{D})R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})}$$

Alors,

$$\begin{aligned} M &= \frac{R(a,\mathbf{C})R(a,\mathbf{D})R(\mathbf{C},\mathbf{D})R((\mathbf{A}\setminus a)\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})R(a,\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},(\mathbf{A}\setminus a)\setminus\mathbf{C})R(\mathbf{C},a)R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})} \\ &= (-1)^p B(a)\frac{R(a,\mathbf{C})R(\mathbf{C},\mathbf{D})R((\mathbf{A}\setminus a)\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},(\mathbf{A}\setminus a)\setminus\mathbf{C})R(a,\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})} \\ &= (-1)^p B(a)\frac{R(\mathbf{C},\mathbf{D})R((\mathbf{A}\setminus a)\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},(\mathbf{A}\setminus a)\setminus\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})} \end{aligned}$$

On pose $\mathbf{C}' = (\mathbf{A}\setminus a)\setminus\mathbf{C}$ et $\mathbf{D}' = \mathbf{B}\setminus\mathbf{D}$; on a $\#\mathbf{C}' = m-1-p = q-1$ et $\mathbf{C}' \subset \mathbf{A}\setminus a$, ainsi que $\#\mathbf{D}' = p$ et $\mathbf{D}' \subset \mathbf{B}$.

$$\begin{aligned} M &= (-1)^p B(a)\frac{R(\mathbf{C}',\mathbf{D}')R((\mathbf{A}\setminus a)\setminus\mathbf{C}',\mathbf{B}\setminus\mathbf{D}')}{R((\mathbf{A}\setminus a)\setminus\mathbf{C}',\mathbf{C}')R(\mathbf{B}\setminus\mathbf{D}',\mathbf{D}')} \\ &= (-1)^p B(a)\frac{(-1)^\alpha R(\mathbf{D}',\mathbf{C}')(-1)^\beta R(\mathbf{B}\setminus\mathbf{D}',(\mathbf{A}\setminus a)\setminus\mathbf{C}')}{(-1)^\gamma R(\mathbf{C}',(\mathbf{A}\setminus a)\setminus\mathbf{C}')(-1)^\delta R(\mathbf{D}',\mathbf{B}\setminus\mathbf{D}')} \end{aligned}$$

avec $\alpha = (q-1)p, \beta = p(q-1), \gamma = p(q-1), \delta = qp$ et $\alpha+\beta+\gamma+\delta = p \pmod 2$. Donc,

$$M = B(a)\frac{R(\mathbf{D}',\mathbf{C}')R(\mathbf{B}\setminus\mathbf{D}',(\mathbf{A}\setminus a)\setminus\mathbf{C}')}{R(\mathbf{C}',(\mathbf{A}\setminus a)\setminus\mathbf{C}')R(\mathbf{D}',\mathbf{B}\setminus\mathbf{D}')}$$

Or,

$$\mathbf{c}_{j-1}(\mathrm{Sylv}^{p,q-1}(\mathbf{B},\mathbf{A}\setminus a)(X)) = \sum_{\substack{\mathbf{C}' \subset_{q-1} \mathbf{A}\setminus a \\ \mathbf{D}' \subset_p \mathbf{B}}} \frac{R(\mathbf{D}',\mathbf{C}')R(\mathbf{B}\setminus\mathbf{D}',(\mathbf{A}\setminus a)\setminus\mathbf{C}')}{R(\mathbf{C}',(\mathbf{A}\setminus a)\setminus\mathbf{C}')R(\mathbf{D}',\mathbf{B}\setminus\mathbf{D}')}$$

Ce qui implique

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = (-1)^p B(a)\mathbf{c}_{j-1}(\mathrm{Sylv}^{p,q-1}(\mathbf{B},\mathbf{A}\setminus a)(X)).$$

3. $j = n = m = p + q$.

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b) = \sum_{\substack{\mathbf{C} \subset_p \mathbf{A} \\ \mathbf{D} \subset_q \mathbf{B}\setminus b}} \frac{R(b,\mathbf{C})R(b,\mathbf{D})R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})}$$

Posons

$$N = \frac{R(b,\mathbf{C})R(b,\mathbf{D})R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},\mathbf{B}\setminus\mathbf{D})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},\mathbf{B}\setminus\mathbf{D})}$$

Alors,

$$\begin{aligned} N &= \frac{R(b,\mathbf{C})R(b,\mathbf{D})R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},(\mathbf{B}\setminus b)\setminus\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},b)}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},b)R(\mathbf{D},(\mathbf{B}\setminus b)\setminus\mathbf{D})} \\ &= \frac{R(b,\mathbf{C})(-1)^q R(\mathbf{D},b)R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},(\mathbf{B}\setminus b)\setminus\mathbf{D})(-1)^q R(b,\mathbf{A}\setminus\mathbf{C})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},b)R(\mathbf{D},(\mathbf{B}\setminus b)\setminus\mathbf{D})} \\ &= A(b)\frac{R(\mathbf{C},\mathbf{D})R(\mathbf{A}\setminus\mathbf{C},(\mathbf{B}\setminus b)\setminus\mathbf{D})}{R(\mathbf{C},\mathbf{A}\setminus\mathbf{C})R(\mathbf{D},(\mathbf{B}\setminus b)\setminus\mathbf{D})} \end{aligned}$$

On pose $\mathbf{C}' = \mathbf{A}\setminus\mathbf{C}$ et $\mathbf{D}' = (\mathbf{B}\setminus b)\setminus\mathbf{D}$; on a $\#\mathbf{C}' = q$ et $\mathbf{C}' \subset \mathbf{A}$, ainsi que $\#\mathbf{D}' = p-1$ et $\mathbf{D}' \subset \mathbf{B}\setminus b$.

$$\begin{aligned} N &= A(b)\frac{R(\mathbf{C}',\mathbf{D}')R(\mathbf{A}\setminus\mathbf{C}',(\mathbf{B}\setminus b)\setminus\mathbf{D}')}{R(\mathbf{A}\setminus\mathbf{C}',\mathbf{C}')R((\mathbf{B}\setminus b)\setminus\mathbf{D}',\mathbf{D}')} \\ &= A(b)\frac{R(\mathbf{C}',\mathbf{D}')R(\mathbf{A}\setminus\mathbf{C}',(\mathbf{B}\setminus b)\setminus\mathbf{D}')}{(-1)^{pq}R(\mathbf{C}',\mathbf{A}\setminus\mathbf{C}')(-1)^{(p-1)q}R(\mathbf{D}',(\mathbf{B}\setminus b)\setminus\mathbf{D}'} \\ &= (-1)^q A(b)\frac{R(\mathbf{C}',\mathbf{D}')R(\mathbf{A}\setminus\mathbf{C}',(\mathbf{B}\setminus b)\setminus\mathbf{D}')}{R(\mathbf{C}',\mathbf{A}\setminus\mathbf{C}')R(\mathbf{D}',(\mathbf{B}\setminus b)\setminus\mathbf{D}')} \end{aligned}$$

Or,

$$\mathbf{c}_{j-1}(\mathrm{Sylv}^{q,p-1}(\mathbf{A},\mathbf{B}\setminus b)(X)) = \sum_{\substack{\mathbf{C}'\subset_q\mathbf{A}\\ \mathbf{D}'\subset_{p-1}\mathbf{B}\setminus b}} \frac{R(\mathbf{C}',\mathbf{D}')R(\mathbf{A}\setminus\mathbf{C}',(\mathbf{B}\setminus b)\setminus\mathbf{D}')}{R(\mathbf{C}',\mathbf{A}\setminus\mathbf{C}')R(\mathbf{D}',(\mathbf{B}\setminus b)\setminus\mathbf{D}'}$$

Donc,

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b) = (-1)^q A(b)\mathbf{c}_{j-1}(\mathrm{Sylv}^{q,p-1}(\mathbf{A},\mathbf{B}\setminus b)(X))$$

■

Preuve de la proposition 2.2.— On fait une double récurrence sur n et m.
Si $n < m$, on considère la propriété $\mathcal{F}_{m,n}$ suivante : pour tous $\mathbf{A}$ et $\mathbf{B}$ de cardinal respectif m et n, et tous p, q tels que $p+q=n$

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X) = (-1)^{p(m-n)}\binom{n}{p}\,B(X).$$

On considère aussi la propriété $\mathcal{G}_n$ suivante : pour tous $\mathbf{A}$ et $\mathbf{B}$ de cardinal n et tous p, q tels que $p+q=n$

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X) = \binom{n-1}{q}\,A(X) + \binom{n-1}{p}\,B(X).$$

– Initialisation.
  – Pour prouver $\mathcal{F}_{m,0}$ avec $m>0$, on remarque que $p+q=n=0$, donc $p=q=0$ et on a d'une part

$$\mathrm{Sylv}^{0,0}(\mathbf{A},\mathbf{B})(X) = R(A,\emptyset) = 1,$$

  d'autre part,

$$(-1)^{p(m-n)}\binom{n}{p}\,B(X) = R(X,\emptyset) = 1.$$

  Ce qui prouve que $\mathcal{F}_{m,0}$ est vraie.
  – Pour prouver $\mathcal{G}_1$, il faut prendre $n = 1 = p+q$.

– si $p = 1$: $\mathrm{Sylv}^{1,0}(\mathbf{A},\mathbf{B})(X) = X - a = A(X)$, et $\binom{n-1}{q} A(X) + \binom{n-1}{p} B(X) = A(X)$, car $\binom{n-1}{p} = \binom{0}{p} = 0$.

– si $q = 1$: $\mathrm{Sylv}^{0,1}(\mathbf{A},\mathbf{B})(X) = B(X)$, et $\binom{n-1}{q} A(X) + \binom{n-1}{p} B(X) = A(X)$, car $\binom{n-1}{q} = \binom{0}{q} = 0$.

– Si $0 < n < m$, montrons $\mathcal{F}_{m,n}$ en supposant $\mathcal{F}_{m-1,n}$ vérifiée ainsi que $\mathcal{G}_n$ Pour tout $a \in \mathbf{A}$,

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = (-1)^p \mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A}\setminus a,\mathbf{B})(X))B(a)$$

(c'est le lemme 2.3, 1)

1er cas. $m-1 > n = p+q$: on applique $\mathcal{F}_{m-1,n}$: $\mathrm{Sylv}^{p,q}(\mathbf{A}\setminus a,\mathbf{B})(X) = (-1)^{p(m-1-n)}\binom{n}{p} B(X)$ et donc

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = (-1)^{p(m-n)}\binom{n}{p} B(a)$$

Les polynômes $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X)$ et $(-1)^{p(m-n)}\binom{n}{p}\mathbf{B}(X)$, qui sont de degré $p+q = n < m$, prennent les mêmes valeurs en les m points de $\mathbf{A}$: ils sont donc égaux.

2ème cas. $m-1 = n = p+q$: il s'agit de montrer $\mathcal{F}_{n+1,n}$. Pour cela, on applique $\mathcal{G}_n$ à $\mathbf{A}\setminus a$ et $\mathbf{B}$ ($\mathbf{A}$ est de cardinal $n+1$ et $\mathbf{B}$ est de cardinal n).

$$\mathrm{Sylv}^{p,q}(\mathbf{A}\setminus a,\mathbf{B})(X) = \binom{n-1}{q}\frac{A(X)}{X-a} + \binom{n-1}{p} B(X).$$

On déduit

$$\mathbf{c}_n(\mathrm{Sylv}^{p,q}(\mathbf{A}\setminus a,\mathbf{B})(X)) = \binom{n-1}{q} + \binom{n-1}{p} = \binom{n}{p}$$

et

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = (-1)^p\binom{n}{p} A(a) = (-1)^{(m-n)p}\binom{n}{p} A(a)$$

la dernière égalité provenant de $m-n = 1$.
On a à nouveau deux polynôme de degré $p+q = n$ qui coïncident aux m points de $\mathbf{A}$, avec $m > n$; ces deux polynômes sont donc égaux.

– Montrons $\mathcal{G}_{n+1}$ lorsque $\mathcal{G}_n$ est vrai : on a alors $\mathcal{F}_{n+1,n}$ (voir ci-dessus).
On calcule pour tout $a \in \mathbf{A}$ et tout $b \in \mathbf{B}$, $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a)$, et $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b)$, qu'on compare à $\left(\binom{n}{q} A + \binom{n}{p} B\right)(a)$ et $\left(\binom{n}{q} A + \binom{n}{p} B\right)(b)$.

– Si $q = 0$: $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X) = A(X)$, $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = 0$ et $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b) = A(b)$;
$\left(\binom{n}{0} A + \binom{n}{n+1} B\right)(a) = 0$ car $\binom{n}{n+1} = 0$;
$\left(\binom{n}{0} A + \binom{n}{n+1} B\right)(b) = A(b)$ car $\binom{n}{n+1} = 0$.

– Si $p = 0, q = n$: $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X) = B(X)$, $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = B(a)$ et $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b) = 0$;
$\left(\binom{n}{n+1} A + \binom{n}{0} B\right)(a) = B(a)$ car $\binom{n}{n+1} = 0$;

$$\left(\binom{n}{n+1} A + \binom{n}{0} B\right)(b) = 0 \text{ car } \binom{n}{n+1} = 0.$$

– Si $p \neq 0$ et $q \neq 0$, d'après le lemme 2.3, 2,

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = (-1)^p B(a)\mathbf{c}_{j-1}(\mathrm{Sylv}^{p,q-1}(\mathbf{B},\mathbf{A}\setminus a)(X))$$

On peut appliquer $\mathcal{F}_{n+1,n}$ au quadruplet $(n+1,n,p,q-1)$ pour $\mathbf{B}$ et $\mathbf{A}\setminus a$. On a donc

$$\mathrm{Sylv}^{p,q-1}(\mathbf{B},\mathbf{A}\setminus a)(X) = (-1)^p \binom{n}{p} B(X)$$

d'où l'on déduit

$$\mathbf{c}_{j-1}(\mathrm{Sylv}^{p,q-1}(\mathbf{B},\mathbf{A}\setminus a)(X)) = (-1)^p \binom{n}{p}.$$

D'où

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = \binom{n}{p} B(a)$$

Par ailleurs,

$$\left(\binom{n}{q} A + \binom{n}{p} B\right)(a) = \binom{n}{p} B(a).$$

De même, d'après le lemme 2.3, 3,

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b) = (-1)^q A(b)\mathbf{c}_{j-1}(\mathrm{Sylv}^{q,p-1}(\mathbf{A},\mathbf{B}\setminus b)(X))$$

On peut appliquer $\mathcal{F}_{n+1,n}$ au quadruplet $(n+1,n,q,p-1)$ pour $\mathbf{A}$ et $\mathbf{B}\setminus b$.

$$\mathrm{Sylv}^{q,p-1}(\mathbf{A},\mathbf{B}\setminus b)(X) = (-1)^q \binom{n}{q} A(X)$$

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(a) = \binom{n}{q} A(b)$$

Par ailleurs,

$$\left(\binom{n}{q} A + \binom{n}{p} B\right)(b) = \binom{n}{q} A(b)$$

Dans ces 3 cas, qui couvrent tous les cas possibles, les deux polynômes $\binom{n}{q} A + \binom{n}{p} B$ et $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})$, qui sont tous les deux de degré $p+q = n+1$, coïncident aux $2(n+1)$ points de $\mathbf{A}$ et $\mathbf{B}$. Ils sont donc égaux.

∎

3 Deux propriétés des sous-résultants.

Les sous-résultants se comportent comme les doubles sommes de Sylvester : on a l'anologue de la proposition 2.1 et de la proposition 2.2, 1.

Proposition 3.1 *Si b est une racine de B, alors, pour tout $0 \leq j < n < m$,*

$$\mathrm{Sres}_j(A,B)(b) = (-1)^{m-j} A(b)\mathbf{c}_j\left(\mathrm{Sres}_j\left(A, \frac{B}{X-b}\right)(X)\right).$$

Preuve.— Démontrons $\mathrm{Sres}_j(A,B)(b) = (-1)^{m-j}A(b)\mathbf{c}_{j+1}\mathrm{Sres}_{j+1}\left((X-b)A,B\right)$.
Supposons tout d'abord que $j < n-1$; on remarque les faits suivants, si $j < n-1$ et $1 \leq \ell \leq n-j-1$:

1. on a :
$$\begin{aligned} X^{n-(j+1)-\ell}(X-b)A &= X^{n-(j+1)-\ell+1}A - bX^{n-(j+1)-\ell}A \\ &= X^{n-j-\ell}A - bX^{n-j-(\ell+1)}A \quad ; \end{aligned}$$
2. si $A = \sum_{k=0}^{m} \alpha_k X^{m-k}$, alors
$$(X-b)A = \alpha_0 X^{m+1} + \sum_{k=1}^{m}(\alpha_k - \alpha_{k-1}b)X^{m+1-k} - \alpha_m b$$

Donc, si, dans la matrice $M_j(A,B)$, pour $1 \leq \ell \leq q-j-1$, on remplace la ℓ-ième ligne L_ℓ par la combinaison linéaire de lignes $L_\ell - bL_{\ell+1}$, on obtient une matrice $M'_j(A,B)$ vérifiant $\det M'_j(A,B) = \det M_j(A,B)$ et dont
– les $(n-1-j)$ premières lignes sont les $(n-1-j)$ premières lignes de $M_{j+1}((X-b)A,B)$;
– les $(m-j) = (m+1-(j+1))$ dernières lignes sont les $(m-j)$ dernières lignes de $M_{j+1}((X-b)A,B)$ (matrice qui a une ligne de moins que la matrice $M_j(A,B)$).
Si on spécialise la matrice $M'_j(A,B)$ en b, (ce qui ne touche qu'à sa dernière colonne), alors, cette dernière colonne présente des zéros partout sauf sur la ligne $n-j$. En position $n-j$, on trouve $A(b)$. On développe le déterminant de $M'(A,B)(b)$ le long de cette dernière colonne, ce qui donne

$$\det(M'_j(A,B)(b)) = \det(M_j(A,B)(b)) = \mathrm{Sres}_j(A,B)(b) = (-1)^{m-j}A(b)\det(N)$$

où N est la matrice obtenue à partir de $M'_j(A,B)$ en supprimant la $(n-j)$-ième ligne et la dernière colonne, ce qui donne exactement $N = \mu_{j+1,j+1}((X-b)A,B)$ et $\det(N) = \mathbf{c}_{j+1}\mathrm{Sres}_{j+1}((X-b)A,B)$. Ce qui termine la preuve dans le cas $j < n-1$.
Si maintenant $j = n-1$, alors $\mathrm{Sres}_{n-1}(A,B)(b) = (-1)^{m-n+1}A(b)$, et $\mathrm{Sres}_n((X-b)A,B)(X) = Q$, donc, $\mathbf{c}_n(\mathrm{Sres}_n(X-b)A,B) = 1$ et $\mathrm{Sres}_{n-1}(A,B)(b) = (-1)^{m-j}A(b)\mathbf{c}_n(\mathrm{Sres}_n(X-b)A,B)$, puisque $j = n-1$.
On a démontré
$$\mathrm{Sres}_j(A,B)(b) = (-1)^{m-j}A(b)\mathbf{c}_{j+1}(\mathrm{Sres}_{j+1}\left((X-b)A,B\right)).$$

Pour obtenir la proposition il suffit d'utiliser

$$\mathrm{Sres}_{j+1}((X-b)A,B)(X) = (X-b)\mathrm{Sres}_j\left(A,\frac{B}{X-b}\right)(X),$$

qui est un cas particulier du point 4 de la remarque 1.2 ∎

Proposition 3.2
$$\mathrm{Sres}_n(A,B)(X) = \varepsilon_{m-n}B(X).$$

Preuve.— La preuve est une conséquence immédiate de la définition des sous-résultants. ∎

Remarque 3.3 Notons qu'il n'y a pas d'équivalent de la proposition 2.2, 2 : les sous-résultants ne sont pas définis pour $n = m$.

Conséquence 3.4 De la proposition 3.1 on déduit, pour $j = n-1$, par interpolation de Lagrange :

$$\begin{aligned}\mathrm{Sres}_{n-1}(A,B)(X) &= \sum_{i=1}^{n}(-1)^{m-n+1}A(b_i)\mathbf{c}_{n-1}\left(A,\frac{B}{X-b}\right)\frac{\prod_{j\neq i}(X-b_j)}{\prod_{j\neq i}(b_i-b_j)}\\ &= \sum_{i=1}^{n}(-1)^{m-n+1}\frac{R(b_i,\mathbf{A})R(X,\mathbf{B}-b_i)}{R(b_i,\mathbf{B}-b_i)}.\end{aligned}$$

ce qui est exactement le théorème principal avec le quadruplet $(m,n,0,n-1)$. En effet, en appliquant ce théorème principal pour ce quadruplet, on a

$$\begin{aligned}\mathrm{Sylv}^{0,n-1}(A,B)(X) &= \sum_{i=1}^{n}\frac{R(X,\mathbf{B}-b_i)R(\mathbf{A},b_i)}{R(\mathbf{B}-b_i,b_i)}\\ &= \sum_{i=1}^{n}\frac{R(X,\mathbf{B}-b_i)(-1)^m R(b_i,\mathbf{A})}{(-1)^{n-1}R(b_i,\mathbf{B}\setminus b_i)}\\ &= \mathrm{Sres}_{n-1}(A,B)(X).\end{aligned}$$

4 Preuve du théorème principal.

Rappelons l'énoncé du théorème, avec les notations ci-dessus.

Théorème 4.1 *Soient $j \leq n < m$ et p,q tels que $p+q=j$, alors*

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(X) = (-1)^{p(m-j)}\varepsilon_{m-j}\binom{j}{p}\,\mathrm{Sres}_j(A,B)(X).$$

Remarque 4.2 À partir de la proposition 3.1 et de la proposition 2.1, avec ces notations, on a les deux égalités similaires suivantes : si $j \leq n-1$, alors

$$\mathrm{Sres}_j(A,B)(b) = (-1)^{m-j}A(b)\mathbf{c}_j(\mathrm{Sres}_j\left(A,\tfrac{B}{X-b}\right)(X)$$

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B})(b) = (-1)^{m-j}A(b)\mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B}\setminus b)(X)).$$

La mise en parallèle de ces deux résultats conduit à la preuve par récurrence sur n du théorème 4.1. En effet, si le théorème est vérifié pour tout $\mathbf{B}_{n-1}$ de cardinal $n-1$, il est vérifié par $\mathbf{B}\setminus b$ pour tout $b \in \mathbf{B}$. Les coefficients dominants de deux polynômes égaux étant égaux. on obtient, par interpolation aux n éléments de $\mathbf{B}$, que le théorème est vrai pour $\mathbf{B}$.

Preuve.— On rappelle que, si $p+q=n<m$,

$$\begin{aligned}\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B}_n)(X) &= (-1)^{p(m-n)}\binom{n}{p}\,B_n(X),\\ \mathrm{Sres}_n(A,B_n)(X) &= \varepsilon_{m-n}B_n(X).\end{aligned}$$

pour toute famille $\mathbf{B}_n$, ceci d'après la proposition 2.2, 1 et la proposition 3.2, ce qui implique le théorème pour $j=n$.

Pour le cas général, on fait une démonstration par récurrence sur n. L'hypothèse de récurrence $\mathcal{H}_n$ est la suivante.

$\forall j < n$, $\forall (p,q) \in \mathbb{N}^2$ avec $j = p+q$, pour toute famille $\mathbf{B}_n$ de cardinal n, si $B_n = R(X, \mathbf{B}_n)$,

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n)(X) = \varepsilon_{m-j}(-1)^{p(m-j)} \binom{j}{p} \mathrm{Sres}_j(A, B_n)(X),$$

La propriété $\mathcal{H}_1$ est vérifiée, car alors $p = q = 0$, $\mathbf{B}_1 = b$,

$$\begin{array}{rcl} \mathrm{Sylv}^{0,0}(\mathbf{A}, b)(X) & = & R(\mathbf{A}, b) = (-1)^m A(b), \\ \mathrm{Sres}_0(A, b)(X) & = & \varepsilon_m R(\mathbf{A}, b) = (-1)^m \varepsilon_m A(b); \end{array}$$

par la remarque 1.1, 2. et la remarque 1.2, 2. D'où, $\mathrm{Sylv}^{0,0}(\mathbf{A}, b)(X) = \varepsilon_m \mathrm{Sres}_0(A, b)(X)$.

Pour montrer $\mathcal{H}_n$, si $j \neq n-1$, on applique $\mathcal{H}_{n-1}$, ce qui donne pour tout $b \in \mathbf{B}_n$

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n \setminus b)(X) = \varepsilon_j(-1)^{p(m-j)} \binom{j}{p} \mathrm{Sres}_j\left(A, \frac{B_n}{X-b}\right)(X).$$

Les coefficients des termes de degré j de ces deux polynômes sont donc égaux. Or, d'après les propositions 2.1 et 3.1, pour tout $b \in \mathbf{B}_n$,

$$\begin{array}{rcl} \mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n)(b) & = & (-1)^{m-j} A(b) \mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n \setminus b)(X)) \\ \mathrm{Sres}_j(A, B_n)(b) & = & (-1)^{m-j} A(b) \mathbf{c}_j\left(\mathrm{Sres}_j\left(A, \frac{B_n}{X-b}\right)(X)\right) \end{array}$$

Donc, pour tout $b \in \mathbf{B}_n$,

$$\begin{array}{rcl} \mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n)(b) & = & (-1)^{m-j} A(b) \varepsilon_{m-j}(-1)^{p(m-j)} \binom{j}{p} \mathbf{c}_j\left(\mathrm{Sres}_j\left(A, \frac{B_n}{X-b}\right)(X)\right) \\ & = & \varepsilon_{m-j}(-1)^{p(m-j)} \binom{j}{p} \mathrm{Sres}_j(A, B_n)(b) \end{array}$$

la première égalité se déduisant de l'hypothèse de récurrence, la deuxième de la proposition 3.1. Les deux polynômes $\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n)(X)$ et $\varepsilon_{m-j}(-1)^{p(m-p-q)} \binom{j}{p} \mathrm{Sres}_j(A, B_n)(X)$, qui sont tous les deux de degré $j < n-1$, coïncident aux n points de B_n, ils sont donc égaux.

Pour montrer $\mathcal{H}_n$ lorsque $j = n-1$, on remarque que le théorème est vrai pour le couple $(\mathbf{A}, \mathbf{B}_n \setminus b)$ et $j = n-1$. Ce qui permet d'écrire

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n \setminus b)(X) = \varepsilon_{m-n-1}(-1)^{p(m-n-1)} \binom{n-1}{p} \mathrm{Sres}_{n-1}\left(A, \frac{B_n}{X-b}\right)(X).$$

Mais d'après la proposition 3.2

$$\mathrm{Sres}_{n-1}\left(A, \frac{B_n}{X-b}\right)(X) = \varepsilon_{m-n-1} \frac{B_n(X)}{X-b}.$$

Donc,

$$\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n \setminus b)(X) = (-1)^{p(m-n-1)} \binom{n-1}{p} \frac{B_n(X)}{X-b}$$

et

$$\mathbf{c}_j(\mathrm{Sylv}^{p,q}(\mathbf{A}, \mathbf{B}_n \setminus b)(X)) = (-1)^{p(m-n-1)} \binom{n-1}{p}.$$

En appliquant la proposition 2.1 et la proposition 3.1 on a

$$\begin{aligned}\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B}_n)(b) &= (-1)^{m-n-1}A(b)(-1)^{p(m-n-1)}\binom{n-1}{p}\\ \mathrm{Sres}_{n-1}(A,B_n)(b) &= (-1)^{m-n-1}A(b)\mathbf{c}_{n-1}\left(\mathrm{Sres}_{n-1}\left(A,\tfrac{B_n}{X-b}\right)(X)\right)\end{aligned}$$

ce qui donne

$$\mathrm{Sres}_{n-1}(A,B_n)(b) = (-1)^{m-n-1}A(b)\varepsilon_{m-n-1}$$

Donc,

$$\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B}_n)(b) = \varepsilon_{m-n-1}(-1)^{m-n-1}\mathrm{Sres}_{n-1}(A,B_n)(b)$$

Les polynômes $\mathrm{Sylv}^{p,q}(\mathbf{A},\mathbf{B}_n)$ et $\varepsilon_{m-n-1}(-1)^{m-n-1}\mathrm{Sres}_{n-1}(A,B_n)$, qui sont tous les deux de degré $p+q=n-1$, coïncident aux n points de $\mathbf{B}$: ils sont donc égaux. ∎

Bibliographie

[1] C. d'Andrea, H Hong, T. Krick, A. Szanto, An Elementary Proof of Sylvester's Double Sums for Subresultants, *Journal of Symbolic Computation* **42-3** (2007).

[2] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in real algebraic geometry*, Springer, 2003.

[3] H. Hong, Subresultants in Roots., *Prépublication.*

[4] A. Lascoux, P. Pragacz, Double Sylvester sums for subresultants and multi-Schur fonctions, *Journal of Symbolic Computation* **35-6** (2003).

[5] J. J. Sylvester, Note on elimination, *Philosophical Magazine* **XVII** (1840).

[6] J. J. Sylvester, A theory of the syzygetic relations of two rational integral functions, *Philosophical Transactions of the Royal Society of London* **CXLIII-III**.